Background

Windows shares are exposed on port 445, and access with the SMB protocol.

Enumerateusing smbmap

A good tool to map available shares from linux is the following way. You can enumerate just one host if you like. Otherwise you can use nmap to scan the network for open smb ports, save those IP:s in a list. And then scane the entire list with smbmap.

Remember that this will check write permission. smbmap checks write-permissions by creating a folder, and the deleting it. Sometimes it is possible to create a folder, but not remove it, then it will leave a folder with some random name. smbmap tells you when this happens, so you need to ask someone with correct privileges to remove it.

Find shares that are accessible for anonymous users:

```
smbmap --host-file hosts.txt > smbmapresults.txt
```

```
smbmap -u domainusername -p 'supersecretpassword' -d domain.local --host-file /home/<user>/Documents/smbmap/hosts.txt > result.txt
```

```
smbmap -u domainusername -p 'supersecretpassword' -d domain.local --host-file /home/<user>/mappashares/testdownload/test2.txt -R -A
```

Enumerate with PowerView

See chapter tools to see how to install PowerSploit.

First we can list all the shares on the domain:

```
# Finding all shares that exists on the domain. Not very useful.
find-domainshare

# Enumerate all shares that the current user has access to
find-domainshare -CheckShareAccess | export-csv domainshares.csv

# If you get another users account you can test what smb-access that users has. You run the command, and a popup lets you insert the
find-domainshare -Credential hackdomain\user
```

However, it might be faster to search for specific files.

```
find-interestingDomainShareFile -Include ('*.pfx','*.cer','*.pvk','*.pem','*.key','*.crt','*.skr','*.txt','*.rtf','*.cnf','*.cf','*.
```

Access the files

From a windows machine on the same network with domain credentials you can use the following to map a network drive.

```
# First just run `net use` to list all the currently mapped network shares
net use
# Then map a share to a specific name, in the case `x`, but it can be anything.
net use x: \\192.168.xx.x\nameofshare
# Now access the share by running this command
x:

# In order to disconnect from the network share you run this command. Delete here refers to deleting the network connection, not the

net use x: /delete
```

Search the files

```
get-childitem -recurse | select-string -pattern "password" -list | Out-file test.txt
```